PEMBUATAN APLIKASI WEB VULNERABILITY SCANNER TERHADAP KELEMAHAN XSS (Cross Site Scripting) MENGGUNAKAN JAVA.

TUGAS AKHIR

Oleh :

M. TRI JOKO
0534010093

JURUSAN TEKNIK INFORMATIKA
FAKULTAS TEKNOLOGI INDUSTRI
UNIVERSITAS PEMBANGUNAN NASIONAL "VETERAN"
JAWA TIMUR
2010

PEMBUATAN APLIKASI WEB VULNERABILITY SCANNER TERHADAP KELEMAHAN XSS (Cross Site Scripting) MENGGUNAKAN JAVA.

TUGAS AKHIR

Diajukan Untuk Memenuhi Sebagian Persyaratan
Dalam Memperoleh Gelar Sarjana Komputer
Jurusan Teknik Informatika

Oleh :

M. TRI JOKO
0534010093

JURUSAN TEKNIK INFORMATIKA
FAKULTAS TEKNOLOGI INDUSTRI
UNIVERSITAS PEMBANGUNAN NASIONAL "VETERAN"
JAWA TIMUR
2010

KATA PENGANTAR

Alhamdulillah, dengan mengucapkan puji dan syukur kehadirat Allah SWT atas rahmat dan hidayah-Nya sehingga penulis dapat menyelesaikan tugas akhir ini dengan judul “PEMBUATAN APLIKASI WEB VULNERABILITY SCANNER TERHADAP KELEMAHAN XSS (Cross Site Scripting) MENGGUNAKAN JAVA “yang merupakan persyaratan dalam memperoleh gelar Sarjana Komputer di Universitas Pembangunan Nasional “VETERAN” Jatim.

Penulis mengucapkan terima kasih yang sebesar-besarnya kepada pihak-pihak yang telah membantu baik materiil maupun dorongan spirituil untuk menyelesaikan penulisan kerja praktek ini, terutama kepada:

1. Orang Tua dan keluarga tercinta serta sayangku nenni sutomo atas motivasi dan doanya sehingga semua yang dikerjakan dapat berjalan lancar.
2. Bapak Prof. Dr. Ir. Teguh Soedarto, MP, selaku Rektor UPN “Veteran” Jatim.
3. Bapak Ir. Bambang Wahyudi, MS, selaku DEKAN FTI UPN “VETERAN” Jatim.
4. Bapak Nur Cahyo Wibowo, S.Kom, M.Kom selaku Kepala Jur. Sistem Informasi, FTI UPN “VETERAN” Jatim.
5. Bapak Basuki Rachmat, S.Si, MT, selaku Kepala Jurusan Teknik Informatika sekaligus Tim Penguji Tugas Akhir Penulis.
6. Bapak Achmad Junaidi, S.Kom, selaku Dosen Pembimbing yang telah meluangkan waktu untuk memberikan bimbingan selama proses pelaksanaan Tugas Akhir penulis.

7. Bapak Chrystia Aji P, S.Kom, selaku Dosen Pembimbing yang telah meluangkan waktu untuk memberikan bimbingan selama proses pelaksanaan Tugas Akhir penulis.
8. *Special to*: Arbi Septiawan (pakde) dan my laptop yang selalu setia menemaniku untuk mengerjakan ini semua..
9. Dosen-dosen Teknik Informatika dan Sistem Informasi, *staff* dan segenap civitas akademika UPN "VETERAN" Jatim.
10. *My best Friends*: Diah, Indri, Rina, Ve, Amey, MIO *Gangster* (Bang Budi abangku tercinta, Broden, Jo2, Faisal, Ringgo, Mr. Craps, Pak Cahyo, Max, and buat semuanya teman-teman UPN).
11. MITRA IT (BGJUNCTION L2-B23), Pak Wahyudi makasih untuk tempatnya, Frangky, Ito yang slalu setia menemani, semua *crew* Yogyafree.net.
12. Teman-teman Perum Marinir Gunung Sari makasih untuk *suport* dan doanya dan Mas Mukhson makasih slalu kasih info.
13. Tidak lupa penulis ucapkan terima kasih kepada teman-teman yang tidak dapat disebutkan satu persatu atas segala bantuannya dalam menyelesaikan Tugas Akhir ini.

Penulis menyadari sepenuhnya masih banyak terdapat kekurangan dalam penulisan Tugas Akhir ini. Oleh sebab itu kritik serta saran yang membangun dari pembaca sangat membantu guna perbaikan dan pengembangan di masa yang akan datang.

Akhirnya dengan ridho Allah penulis berharap semoga Tugas Akhir ini dapat memberikan manfaat bagi pembaca sekalian terutama mahasiswa di bidang komputer.

Surabaya, 10 Agustus 2010

Penulis

DAFTAR ISI

Halaman

DAFTAR TABEL

Halaman

DAFTAR GAMBAR

Halaman

ABSTRAKSI

Hingga saat ini tindakan penyerangan pada suatu web semakin tinggi. Sering terlihat di media cetak,dan media elektronik begitu banyak berita yang memuat aksi-aksi penyerangan terhadap suatu situs web. Salah satu contoh faktor timbulnya tindakan hacking adalah kesalahan dalam scripting pembuatan web adalah hal terbanyak yang dimanfaatkan oleh para attacker, sehingga rata-rata web yang berhasil diserang melalui lubang ini. Kelemahan-kelemahan scripting yang ditemukan pada proses vulnerabilities scanning misalnya, XSS.

Untuk mencegah tindakan tersebut dapat menggunakan jasa perusahaan audit keamanan web. Dan tentunya akan menghabiskan banyak biaya, untuk menghindari hal tersebut, dalam proyek akhir ini akan dibangun aplikasi web vulnerability scanner yang berfungsi untuk mendeteksi suatu kelemahan web terhadap kelemahan XSS.

Maka dengan menggunakan aplikasi web vulnerability scanner dapat dideteksi suatu kelemahan web terhadap kelemahan XSS dengan lebih dini sehingga dapat dicegah. Untuk kedepannya aplikasi web vulnerability scanner dapat digabungkan dengan browser.

Kata kunci *: XSS ,Web Vulnerability Scanner Java.*

BAB I
PENDAHULUAN

1.1 LATAR BELAKANG

Perkembangan dalam dunia maya terjadi sangat pesat. Teknologi baru dirancang dan diimplementasikan untuk memenuhi kebutuhan pengguna yang semakin beragam. Teknologi halaman *web* termasuk didalamnya. Teknologi yang ada kini telah ber-revolusi menuju ke tingkatan yang berbeda. Halaman *web* kini tidak lagi statis namun juga dinamis. Kini halaman *web* yang dinamis merupakan pemandangan yang biasa kita lihat ketika melakukan *surfing* menggunakan *internet*.

Halaman *web* yang dinamis merupakan teknologi yang memberi perubahan penyediaan informasi, layanan, dan tampilan secara signifikan. Halaman *web* yang dinamis memungkinkan interaksi yang lebih baik antara penyedia layanan dengan penggunanya. Dengan menggunakan teknologi ini, halaman *web* akan terlihat lebih manusiawi. Penyedia layanan dapat menambahkan content-content yang sebelumnya masih merupakan impian belaka.

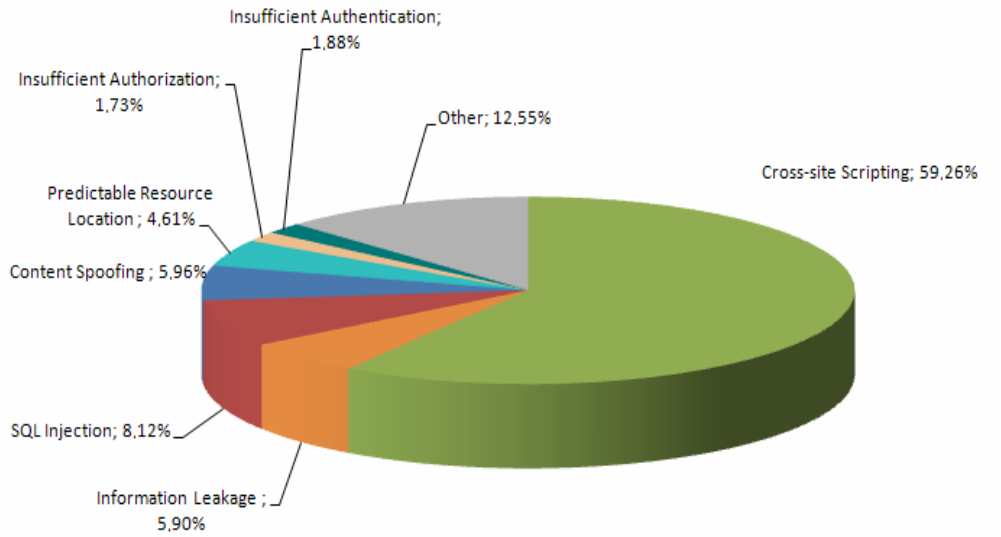
Dalam *system security computer*, istilah *Vulnerability* merupakan suatu kelemahan yang memungkinkan seseorang untuk masuk dan mendapatkan hak akses ke dalam komputer yang dituju(target). Biasanya *vulnerability* adalah kelemahan yang dikarenakan kesalahan setting ataupun ataupun ketidaktahuan administrator.(http://ahmad-prayitno.com)

Dan hingga saat ini angka kejahatan di dunia maya tetap tinggi dan terus meningkat. Sebuah penelitian yang dilakukan oleh *Corsaire* menunjukkan bahwa sekitar 25% aplikasi berbasis *web* memiliki celah yang membuatnya jadi rentan terhadap serangan yang dilakukan oleh para *cracker*. *Corsaire* mendasarkan hasil temuan ini pada penelitian selama enam tahun terakhir. (http://berita.kapanlagi.com)

Dalam menganalisa, *Corsaire* menggunakan sampel dari perusahaan-perusahaan besar di beberapa tempat termasuk *Inggris, Australia, Eropa, Asia* dan tentu saja Amerika Serikat. Hasil analisa menunjukkan bahwa meski ada usaha

untuk memperbaiki aplikasi berbasis *web* ini, namun setidaknya masih ada sekitar 25% yang memiliki resiko tinggi.

Berikut merupakan data dari http://www.webappsec.org/projects/statistics tentang statistic serangan terhadap Aplikasi Web:



Gambar 1. 1 *Data Statistik Serangan terhadap Aplikasi Web*

Dari statistik diatas diketahui bahwa serangan *XSS* menempati urutan Pertama. Para *hacker* berkonsentrasi melakukan *eksploitasi* pada *web-web* di *internet*. *Web* yang tidak aman memberikan kemudahan akses kepada *hacker* untuk memanipulasi informasi dan melakukan aktivitas ilegal dengan menggunakan *situs* yang telah diserang. *Situs* yang menjadi korban dapat disalahgunakan untuk melakukan aktivitas kriminal. Misalnya saja melakukan *phishing*, pencurian informasi sensitif milik pengguna, memanen *email* pengguna untuk keperluan *spamming*, dll. Dalam kondisi ini, *Attacker* dapat membuat agar pemilik sah-nya yang bertanggung jawab atas tindak kejahatan tersebut

Dilatarbelakangi permasalahan di atas, dalam proyek akhir ini dibangun sebuah aplikasi yang berfungsi sebagai pendeteksi terhadap kelemahan *XSS* pada suatu aplikasi *web*, sehingga dengan bantuan aplikasi tersebut suatu aplikasi *web* dapat dideteksi lebih dini terhadap kelemahan *XSS*.

Selain itu, aplikasi ini juga memberikan info letak kelemahan suatu *web* terhadap serangan *XSS*. Dengan aplikasi ini, pengguna bisa mendeteksi apakah *web* memiliki kelemahan *XSS* atau tidak.

1.2 RUMUSAN MASALAH

Dari latar belakang masalah yang telah penulis paparkan, maka penulis mencoba untuk membangun aplikasi *Web Vulnerability Scanner*. Adapun beberapa rumusan permasalahan yang ada dalam membangun aplikasi *Web Vulnerability Scanner* ini yaitu :

a) Bagaimana membangun ***Web Vulnerability Scanner*** berdasarkan data masukan dari pengguna berupa *URL* untuk *Web Vulnerability Scanner* berbasis *Online*.
b) Bagaimana membangun ***Web Vulnerability*** **Scanner** berbasis *Offline* dengan ketentuan *file web* sudah harus tersimpan di *htdocs Xampp*.
c) Bagaimana **Mengolah informasi dan menampilkan hasil scan** yang dibutuhkan oleh pengguna.

1.3 BATASAN MASALAH

Sedangkan batasan masalah pada proyek akhir ini, antara lain :

a) Bahasa yang digunakan adalah *Java* dan *software development*nya adalah Netbeans
b) Aplikasi *web* yang dapat di scan adalah aplikasi *web* yang dibangun dengan menggunakan bahasa pemrograman *PHP* dengan *MYSQL* sebagai *DBMS.*
c) Kelemahan yang dibahas adalah *XSS*

1.4 TUJUAN

Tujuan proyek akhir ini adalah untuk membangun aplikasi *Web Vulnerability Scanner* Menggunakan *Java*. Adapun manfaat dengan dibangunnya aplikasi ini adalah untuk mendeteksi kelemahan *web* terhadap serangan *XSS (Cross Site Scripting).*

1.5 MANFAAT

Berdasarkan dari latar belakang diatas maka dapat dirumuskan masalah sebagai berikut :

a. Membangun *web* secara *secure*.

Membuat *website* dengan tingkat kemanan yang tinggi sehingga tidak mudah untuk dirusak atau dimasuki oleh pihak – pihak tertentu.

b. Terhindar dari *defacer website*.

Adalah bebas dari para perusak tampilan pada *website* yang telah dibangun, bahkan menghapus seluruh data yang ada di dalam *database*.

c. Mendeteksi kelemahan *web* terhadap serangan *XSS (Cross Site Scripting).*

Yaitu mendeteksi salah satu jenis serangan *web* yang dilakukan dengan memanfaatkan kelemahan pada suatu aplikasi *web* sehingga memungkinkan aplikasi untuk menginjeksikan suatu tag *HTML* ataupun *Client Side Script* pada aplikasi *web* tersebut dikarenakan adanya variabel yang tidak disanitasi dengan baik.

1.6 METODOLOGI PENELITIAN

Dalam pengerjaan proyek akhir ini meliputi langkah-langkah sebagai berikut :

1. **Studi Literatur**

   Pada tahap ini dilakukan studi literatur dari beberapa referensi baik itu dari buku atau internet.

2. **Perancangan Sistem**

   Pada tahap ini dilakukan perancangan sistem yang akan dibangun, meliputi perancangan *database*, perancangan sistem dan pembuatan *user interface*.

3. **Persiapan Data**

   Data-data penunjang yang didapatkan berupa suatu kesimpulan, fakta-fakta dan aturan yang mengatur proses pencarian data yang saling berhubungan satu sama lain disimpan ke dalam basis *data RMS (Record Management System)* sebagai media penyimpanan.

4. **Pengujian dan Analisa**

   Pengujian dan analisa dimaksudkan untuk mengetahui sejauh mana sistem yang dibuat pada proyek akhir ini dapat berfungsi sesuai dengan proses sistem yang diharapkan.

5. **Kesimpulan**

Dibuat kesimpulan dari pengujian sistem proyek akhir dengan membandingkan apakah hasilnya seperti yang diharapkan pada tujuan proyek akhir sebelumnya.

6. **Pembuatan Laporan**

   Membuat dokumentasi dari semua tahapan proses diatas berupa laporan yang berisi tentang dasar teori, hasil proyek akhir dan hasil analisa.

1.7 SISTEMATIKA PENELITIAN

Sistematika pembahasan yang akan diuraikan dalam buku laporan proyek akhir ini terbagi dalam beberapa bab yang akan dibahas sebagai berikut :

BAB I PENDAHULUAN

Bab ini berisi tentang pendahuluan yang terdiri dari latar belakang, perumusan masalah, batasan masalah, tujuan dan sasaran, metodologi, serta sistematika pembahasan dari Proyek Akhir ini.

BAB II TEORI PENUNJANG

Bab ini membahas mengenai teori-teori yang berkaitan dengan penyelesaian Proyek Akhir, yang didapatkan dari berbagai macam buku serta sumber-sumber terkait lainnya yang berhubungan dengan pembuatan Proyek Akhir ini.

BAB III PERANCANGAN SISTEM

Bab ini membahas mengenai perancangan sistem, meliputi perancangan hirarki, perancangan proses, dan perancangan *user interface*.

BAB IV IMPLEMENTASI

Bab ini membahas mengenai implementasi system

BAB V UJI COBA DAN ANALISA

Bab ini menyajikan dan menjelaskan seluruh hasil dan analisa dalam pembuatan Proyek Akhir ini dan bagaimana penyelesaian dari setiap permasalahan error yang terjadi pada sistem operasi Windows

BAB VI PENUTUP

Bab ini berisi kesimpulan dari uji coba perangkat lunak, dan saran untuk pengembangan, perbaikan serta penyempurnaan terhadap aplikasi yang telah dibuat.